(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
10. Juni 2004 (10.06.2004)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2004/049159 A2

(51) Internationale Patentklassifikation[7]: G06F 11/22

(21) Internationales Aktenzeichen: PCT/EP2003/012630

(22) Internationales Anmeldedatum:
12. November 2003 (12.11.2003)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
102 54 788.2 22. November 2002 (22.11.2002) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **CONTINENTAL TEVES AG & CO. OHG** [DE/DE]; Guerickestrasse 7, 60488 Frankfurt/Main (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **TRASKOV, Adrian** [DE/DE]; Hardtbergstrasse 8, 61449 Steinbach (DE). **KIRSCHBAUM, Andreas** [DE/DE]; Parsevalstrasse 1, 64347 Griesheim (DE). **EHRENBERG, Thorsten** [DE/DE]; Wettertalstrasse 10, 61231 Bad Nauheim (DE). **KIRSCH, Tasso** [DE/DE]; Odenwaldstrasse 32, 65439 Flörsheim-Wicker (DE). **VOSS, Burkart** [DE/DE]; Hofmannstrasse 6, 64283 Darmstadt (DE).

(74) Gemeinsamer Vertreter: **CONTINENTAL TEVES AG & CO. OHG**; Guerickestrasse 7, 60488 Frankfurt/Main (DE).

(81) Bestimmungsstaaten *(national)*: DE, JP, US.

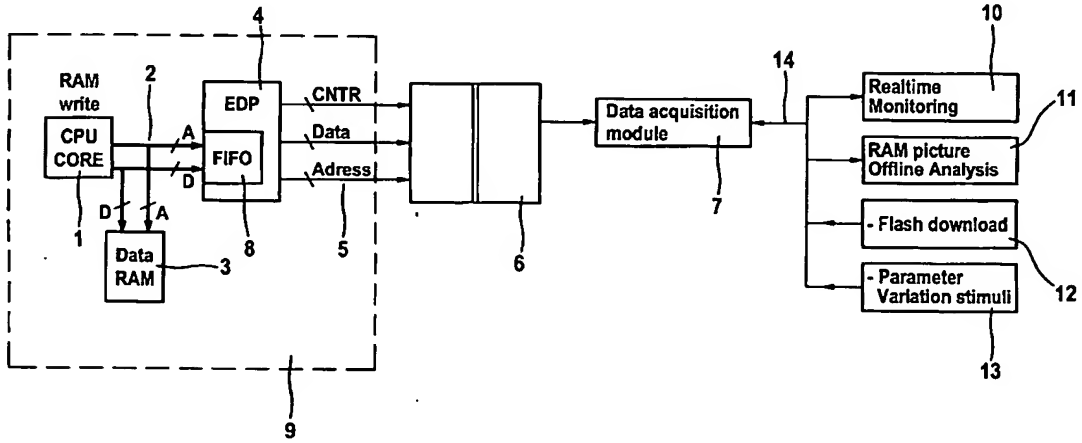
(84) Bestimmungsstaaten *(regional)*: europäisches Patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR).

Veröffentlicht:
— *ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts*

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

(54) Title: DEVICE AND METHOD FOR ANALYSING EMBEDDED SYSTEMS

(54) Bezeichnung: EINRICHTUNG UND VERFAHREN ZUR ANALYSE VON EINGEBETTETEN SYSTEMEN



(57) Abstract: The invention relates to an analysis device for an embedded system (9) comprising a CPU (1), a CPU bus (2) and a memory (3). The embedded system has at least one communication module (4) for the input or output of analysis data via a test interface (5). The communication module permits the internal memory and the input and output access operations of the embedded system to be monitored and/or logged without using the clock cycles of the CPU (1).

(57) Zusammenfassung: Beschrieben ist eine Analyseeinrichtung für ein eingebettetes System (9), welches eine CPU (1), einen CPU-Bus (2) und einen Speicher (3) umfasst. Das eingebettete System weist zumindest ein Kommunikationsmodul (4) für die Ein- bzw. Ausgabe von Analysedaten über eine Testschnittstelle (5) auf. Mit dem Kommunikationsmodul kann ohne Verbrauch von Taktzyklen der CPU (1) der interne Speicher und I/O-Zugriffe des eingebetteten Systems überwacht und/oder protokolliert werden.

WO 2004/049159 A2

Einrichtung und Verfahren zur Analyse von eingebetteten Systemen

Die Erfindung betrifft eine Analyseeinrichtung gemäß Oberbegriff von Anspruch 1, ein eingebettetes System gemäß Oberbegriff von Anspruch 12 sowie ein Verfahren zur Analyse eines eingebetteten Systems mit einer Analyseeinrichtung.

Um Software für eingebettete Systeme erfolgreich entwickeln zu können, ist es allgemein üblich, Einrichtungen vorzusehen, mit denen eine Fehlererkennung zur Laufzeit (Debugging) möglich ist. Bei dem bekannten Konzept des Debugging von eingebetteten Systemen via einer sogenannten JTAG-Schnittstelle (Joint Test Action Group, IEEE Standard 1149.1-1990, "IEEE Standard Test Access Port and Boundary Scan Architecture", Institute of Electrical and Electronics Engineers Inc., New York, USA, 1990)lassen sich Prüfoperationen durch ein "Boundary-Scan"-Testverfahren durchführen. Dieses Verfahren ermöglicht eine Einzelschrittverarbeitung des Prozessors (Singlestepping), das Setzen von Haltepunkten (Breakpoints) und das Setzen von sogenannten Watchpoints. Durch diese an sich bekannten Hilfsmittel zur Fehlererkennung kann zwar die prinzipielle Programmabarbeitung und der Zustand vereinzelter Variablenwerte mitverfolgt werden, jedoch muss das laufende System dazu in der Regel angehalten werden. Nachteilhafterweise kann dann jedoch die Ausgabe des Mikrorechners nicht mehr in Echtzeit erfolgen.

Es besteht nun das Problem, dass eingebettete Systeme häufig Echtzeitsysteme sind, die aufgrund ihres typischen Einsatzgebiets in Echtzeit-Steuerungen/-Regelungen ein Anhalten zu Debuggingzwecken zumindest zur Überprüfung der im Zusammenhang mit der Echtzeitbearbeitung veränderten Daten nicht erlauben.

Weiterhin bekannt ist das sogenannte Trace-Interface, bei dem unter Benutzung eines "Bond-out" Chips zur Echtzeitanalyse die Weiterleitung aller relevanten CPU-Bussignale (Adressen-, Daten-, und Kontrollsignale) über Gehäusepins zum Beispiel an eine externe Logikanalyseeinrichtung ermöglicht wird. Bei einem Bond-out Chip handelt es sich um einen Microcontroller (MCU) in einem anderen Gehäuse, bei dem der Prozessorbus (Daten-, Adressen- und Kontrollsignale) nach außen gebondet ist.

Bei den heute für eingebettete Systeme üblichen hohen Systemfrequenzen von mehreren hundert Megahertz und den modernen Speicherarchitekturen mit Caches kann diese Methode zur Fehleranalyse auf Grund der hohen Geschwindigkeitsanforderungen nicht mehr verwendet werden. Eine Echtzeitausgabe relativ großer Datenspeicher (zum Beispiel einer Größe von mehr als 100 Kbyte) ist in der Regel durch die auf Grund der verwendeten Technologie vorgegebenen Systemfrequenzen und der sich daraus ergebenden Bandbreite nicht möglich. Eine denkbare Möglichkeit zur Schaffung der für die Echtzeitdatenübertragung notwendigen Bandbreite wäre eine parallele Ausgabe der zu übertragenden Daten. Die hierfür zur Verfügung stehende Pinzahl ist jedoch nicht zuletzt aus Kostengründen in der Regel begrenzt.

Aufgabe der vorliegenden Erfindung ist es daher, eine Analyseeinrichtung für eingebettete Systeme zur Verfügung zu stellen, welche auch bei den heute üblichen schnellen eingebetteten Systemen eingesetzt werden kann.

Diese Aufgabe wird durch die Analyseeinrichtung gemäß Anspruch 1 gelöst.

Die Erfindung basiert auf folgenden Überlegungen: Zum einen lässt sich der interne Systemzustand eines eingebetteten Systems durch seinen aktuellen Datenspeicherinhalt (RAM) beschreiben bzw. analysieren. Daraus folgt, dass für den Fall, dass dieser Speicherinhalt in Echtzeit in einen externen Datenspeicher kopiert werden kann, eine Möglichkeit besteht, den Systemzustand von dort durch eine nachgeschaltete Auswerteeinheit weiterzuverarbeiten und auszuwerten.

In der Analyseeinrichtung wird bevorzugt eine Kopie des internen Systemzustands in einen externen Speicher in Echtzeit geschrieben.

Die Analyseeinrichtung ist vorzugsweise Bestandteil eines eingebetteten Systems, welches insbesondere in elektronischen Steuergeräten für Kraftfahrzeugbremssysteme Verwendung findet. In dem eingebetteten System nach der Erfindung sind vorzugsweise wesentliche Komponenten des Systems, wie z.B. eine oder mehrere CPU´s und Speicher teil- oder vollredundant ausgeführt. Hierdurch wird die Betriebssicherheit des eingebetteten Systems erhöht.

Vorzugsweise erfolgt die Protokollierung der Daten nicht in der Weise, dass der gesamte Speicherinhalt oder der Inhalt eines ganzen Speicherbereichs übertragen wird, sondern es werden nur die Veränderungen des Speichers, insbesondere alle Schreibzugriffe der CPU und/oder der Peripherie, übertragen. Auf diese Weise kann eine Verringerung der notwendigen Bandbreite zur Datenausgabe erfolgen.

Das System umfasst außerdem vorzugsweise Mittel für die direkte Datenausgabe durch die CPU. Neben diesen Mitteln für die direkte Datenausgabe sind insbesondere Mittel für eine automatische Replizierung der Daten im Hintergrund durch das

Analysemodul vorgesehen. Hierdurch ergibt sich der Vorteil einer erhöhten Flexibilität bei der Datenausgabe.

Speziell für diese Anwendungsfälle wird gemäß der Erfindung ein universelles Datenein- und ausgabemodul vorgeschlagen, welches in der Weise eingerichtet ist, dass in Echtzeit ein Datenaustausch mit einem eingebetteten System durchgeführt werden kann, ohne dass dieses (auch nur zeitweise) angehalten werden muss (non-intrusive).

Gegenüber den aus dem Stand der Technik bekannten Software-Debuggingeinrichtungen besitzt die Analyseeinrichtung nach der Erfindung den Vorteil, dass bei der Entwicklung von Regelalgorithmen z. B. für Kraftfahrzeugbremssysteme, das dynamische Systemverhalten insbesondere der Regelvariablen während des Debuggings verfolgt werden kann. Weiterhin ist vorteilhaft, dass für den Einsatz eines eingebetteten Systems in einem Hardware-in-the-Loop Simulator oder in einem Rapid-Prototyping System eine Dateneingabe in das eingebettete System vorgenommen werden kann.

Die Erfindung betrifft weiterhin ein Verfahren zur Analyse eines dem weiter oben beschriebenen eingebetteten System mit einer Analyseeinrichtung gemäß Anspruch 12.

Das Verfahren hat den Vorteil, dass die Verarbeitungsgeschwindigkeit des eingebetteten Systems durch die im Hintergrund ablaufenden Debugging-Prozesse nicht verringert wird. Hierdurch ist eine Echtzeitverarbeitung der Daten auch während des Debuggings möglich.

Das Verfahren gemäß der Erfindung umfasst bevorzugt auch Schritte zur echtzeitfähigen Ausgabe des kompletten Datenspeicherinhalts.

Weitere bevorzugte Ausführungsformen ergeben sich aus den Unteransprüchen.

Nachfolgend wird die erfindungsgemäße Analyseeinrichtung und das erfindungsgemäße Verfahren an Hand von Ausführungsbeispielen unter Bezugnahme auf Fig. 1 beschrieben.

Fig. 1 zeigt ein eingebettetes System 9 mit einer Analyseeinrichtung 4 gemäß der Erfindung.

Eingebettetes System 9 umfasst einen oder mehrere CPU´s 1, ein RAM 3, eine Analyseeinrichtung 4 und ein Debugg-Interface 5. Zur Vereinfachung des Blockschaltbilds sind weitere übliche Funktionselemente des eingebetteten Systems, wie ROM, Takterzeugung, IO, etc., nicht gezeichnet.

Die Analyseeinrichtung weist drei Funktionsmodi auf, welche nachfolgend beschrieben werden. In Funktionsmodus 1 liest die Analyseeinrichtung alle Schreibzugriffe der CPU 1 vom Datenspeicher 3 mit. Es werden also alle Schreibzugriffe der CPU 1 auf Datenspeicher 3 automatisch über CPU-Bus 2 von der vorgeschlagenen erweiterten Datenaus-/eingabeeinheit 4 (EDP, Enhanced Data Port) mittels eines darin enthaltenen Controllers über ein paralleles Interface 5 auf den externen Datenspeicher 6 geschrieben. Hierzu muss der Controller zumindest die gleiche Bandbreite besitzen, wie der verwendete Speicher 3. Der Controller besitzt neben einer Verbindung zum Datenbus auch insbesondere eine Verbindung zum Kontrollbus und zum Adressbus, damit, nach einer bevorzugten Ausführungsform des Verfahrens, nur speziell selektierte Adressbereiche und/oder speziell selektierte Datentypen für die Analyse mitverfolgt werden können. Für den Abgriff der Daten und den

Datentransfer muss CPU 1 demzufolge keine zusätzlichen Befehle ausführen.

Der externe Datenspeicher 6 ist bevorzugt als Dual-Port Speicher ausgeführt und enthält in der Regel ein genaues Abbild der in RAM 3 beobachteten Speicherbereiche bzw. des gesamten Speicherinhaltes von RAM 3. Es kann sich bei Speicher 6 auch um einen Ringspeicher handeln, der den ankommenden Datenstrom für eine spätere (offline-) Analyse speichert.

Externes Interface 5 weist bevorzugt eine Bandbreite auf, die kleiner ist als die Bandbreite des CPU-Bus. FIFO-Speicher 8, welcher innerhalb der Datenausgabeeinheit 4 angeordnet ist, sorgt dabei für eine zeitliche Pufferung der abgegriffenen Daten. Auf diese Weise können auch Zugriffe auf Interface 5 ausgegeben werden, bei denen ein Zurückschreiben einer Cache-Line oder eines CPU-Register Dump bei Funktionseintritt durchgeführt wird.

In Funktionsmodus 2 liest Analyseeinrichtung 4 alle Lesezugriffe von CPU 1 auf den Datenspeicher mit. Dieser Modus entspricht weitgehend Funktionsmodus 1, jedoch sind folgende Unterschiede vorhanden: Alle Lesezugriffe werden automatisch über Interface 5 ausgegeben. Analyseeinheit 4 registriert dabei alle Vorgänge, wie Lesezyklen, Schreibzyklen etc., die auf dem CPU-Bus sichtbar sind, auf (Mitlesen). In Funktionsmodus 2 führt CPU 1 aktiv einen Speicherdump durch, was allerdings mit einem geringfügigen tolerierbaren Laufzeitverlust einhergeht. Durch das Mitlesen der Analyseeinheit 4 werden die Anzahl von Taktzyklen, welche für die Ausgabe die von Datenworten zur Analyse erforderlich sind, verringert bzw. oder sogar ganz vermieden.

CPU 1 liest den Datenspeicherinhalt in die nichtgezeichneten Register der CPU ein. Die in den Registern vorhandenen Daten können dann in Analyseeinheit 4 geschrieben werden. Die hier beschriebene Funktionsweise entspricht im wesentlichen dem weiter unten beschriebenen Funktionsmodus 3.

Bei der im vorliegenden Beispiel (Funktionsmodus 2) vorgeschlagenen Analyseeinrichtung liest CPU 1 den Datenspeicherinhalt in die CPU-Register. Parallel hierzu gibt die Datenausgabeeinheit 4, welche den Datenbus mithört, die entsprechenden Daten automatisch aus, d.h. es ist kein expliziter Schreibzyklus für die Datenausgabe zur Analyse erforderlich.

In Funktionsmodus 3 erfolgt ein direktes Schreiben auf die Datenausgabeeinheit oder ein direktes Lesen von der Datenausgabeeinheit. Funktionsmodus 3 entspricht also Funktionsmodus 1, bis auf die Tatsache, dass die Daten aktiv durch die CPU 1 auf die Analyseeinheit 4 extern ausgegeben bzw. aktiv von dort eingelesen werden, wodurch allerdings zusätzliche Taktzyklen erforderlich sind.

Die Analyseeinheit kann über Modul 7 Daten aus dem externen Speicher 6 an typische Debugging-Anwendungen, wie z.B. Echtzeitüberwachung des Systemzustands 10, Offline-Analyse zur Schaffung eines kompletten Datenspeicherabbilds über Modul 11, Flash-Download über Kommunikationskanal 12 (Programmierung des Programmspeichers), Parametervariation während des Betriebs des eingebetteten Systems, Übertragung von Systemstimuli, Rapid-Prototyping und Hardware-in-the-Loop Simulation übertragen werden.

Patentansprüche

1. Analyseeinrichtung für ein eingebettetes System (9), welches eine CPU (1), einen CPU-Bus (2) und einen Speicher (3) umfasst, wobei diese zumindest ein Kommunikationsmodul (4) für die Ein- bzw. Ausgabe von Analysedaten über eine Testschnittstelle (5) aufweist, dadurch **gekennzeichnet**, dass mit dem Kommunikationsmodul ohne Verbrauch von Taktzyklen der CPU (1) der interne Speicher und I/O-Zugriffe des eingebetteten Systems überwacht und/oder protokolliert werden kann.

2. Analyseeinrichtung nach Anspruch 1, **gekennzeichnet** durch zwei, insbesondere mindestens drei frei wählbare Analysemodi, wobei sich die Analysemodi in Art und Umfang der Beteiligung der CPU 1 beim Einlesen und/oder Schreiben von Daten für Analysezwecke voneinander unterscheiden.

3. Analyseeinrichtung nach Anspruch 2, dadurch **gekennzeichnet**, dass je nach gewähltem Analysemodus entweder

   - alle Schreibzugriffe der CPU auf insbesondere definierbare Adressbereiche ohne Taktzyklenverbrauch protokolliert werden oder

   - alle Lesezugriffe der CPU protokolliert werden oder

   - ein direktes Lesen und Schreiben der CPU aus/in einem/-n externen Speicher (6) mit Taktzyklenverbrauch erfolgt.

4. Analyseeinrichtung nach mindestens einem der Ansprüche 1 bis 3, dadurch **gekennzeichnet**, dass das Kommunikationsmodul einen Controller umfasst, welcher selbstständig über eine Verbindung mit dem Datenbus und/oder dem Kontrollbus und/oder dem Adressbus auf diese(n) Bus/Busse des eingebetteten Systems zugreifen kann, um Schreib- und/oder Lese-Zugriffe in Echtzeit, d.h. ohne Beeinflussung der CPU, mitzuverfolgen.

5. Analyseeinrichtung nach mindestens einem der Ansprüche 1 bis 4, dadurch **gekennzeichnet**, dass das Kommunikationsmodul mit einem Pufferspeicher (8) verbunden ist oder diesen insbesondere umfasst, wobei in dem Pufferspeicher die bei Schreib- und/oder Lese-Zugriffen übertragenen Daten gespeichert werden können.

6. Analyseeinrichtung nach mindestens einem der Ansprüche 1 bis 5, dadurch **gekennzeichnet**, dass aus dem Pufferspeicher Daten über die Testschnittstelle (5) gepuffert ausgegeben bzw. Daten in den Pufferspeicher über diese Schnittstelle eingeschrieben werden können.

7. Analyseeinrichtung nach mindestens einem der Ansprüche 1 bis 6, dadurch **gekennzeichnet**, dass der externe Prüfspeicher (6) ein Ringspeicher oder ein Dual-Port Speicher ist.

8. Analyseeinrichtung nach mindestens einem der Ansprüche 1 bis 7, dadurch **gekennzeichnet**, dass das Kommunikationsmodul (4) im eingebetteten System integriert ist.

9. Analyseeinrichtung nach mindestens einem der Ansprüche 1 bis 8, dadurch **gekennzeichnet**, dass die Testschnitt-

stelle (5) mit einem außerhalb des eingebetteten Systems angeordneten Prüfspeicher (6) verbunden ist.

10. Analyseeinrichtung nach mindestens einem der Ansprüche 1 bis 9, dadurch **gekennzeichnet**, dass die Datenübertragung vom Kommunikationsmodul zum externen Speicher über eine Parallelschnittstelle erfolgt.

11. Analyseeinrichtung nach mindestens einem der Ansprüche 1 bis 10, dadurch **gekennzeichnet**, dass externer Speicher (6) mit einer Datenaufbereitungseinrichtung (7) verbunden ist, welche eine Schnittstellenverbindung (14) zu externen Debugging-Anwendungen schafft.

12. Eingebettetes System umfassend eine Zentralrecheneinheit (1), einen CPU-Bus (2) und einem Speicher (3), dadurch **gekennzeichnet**, dass dieses eine Analyseeinrichtung gemäß mindestens einem der Ansprüche 1 bis 11 umfasst.

13. Verfahren zur Analyse eines eingebetteten Systems mit einer Analyseeinrichtung, gemäß mindestens einem der Ansprüche 1 bis 11, dadurch **gekennzeichnet**, dass mindestens ein Modus vorhanden ist, in dem die Analysedaten in Echtzeit aus dem System, welches zumindest CPU, Datenspeicher, Programmspeicher und I/O-Element/-e umfasst, herausgelesen und/oder in das System hinein geschrieben werden können, so dass das System für die Analyse nicht angehalten bzw. unterbrochen werden muss.

14. Verfahren nach Anspruch 13, dadurch **gekennzeichnet**, dass

- der Speicherinhalt oder eine entsprechend auswertbare Information des eingebetteten Systems ganz oder teilweise in einen externen Speicher in Echtzeit kopiert wird, wobei insbesondere zuvor die Daten gepuffert werden, und/oder

- der Speicherinhalt eines externen Speichers (6) oder eine entsprechend auswertbare Information über den Speicherinhalt von Speicher (6) ganz oder teilweise in einen Speicher des eingebetteten Systems in Echtzeit kopiert wird, wobei insbesondere zuvor die Daten gepuffert werden.

15. Verfahren nach Anspruch 13 oder 14, dadurch **gekennzeichnet**, dass der externe Speicher zur Übertragung von Daten für typische Debugging-Anwendungen verwendet wird.

16. Verfahren nach mindestens einem der Ansprüche 13 bis 15, dadurch **gekennzeichnet**, dass nur die für das Debugging erforderlichen Daten bei Zugriffen der CPU auf RAM 3 an den externen Speicher (6) übertragen werden.

17. Verfahren nach mindestens einem der Ansprüche 13 bis 16, dadurch **gekennzeichnet**, dass Schreibzugriffe und/oder Lesezugriffe der CPU mittels eines Pufferspeichers protokolliert werden.

18. Verfahren nach Anspruch 13 bis 17, dadurch **gekennzeichnet**, dass Informationen über die Schreibzugriffe ohne zusätzliche CPU-Befehle in den Pufferspeicher (8) oder direkt in das Kommunikationsmodul (4) geschrieben werden und die Informationen über die Lesezugriffe mit aktiver Unterstützung der CPU in den Pufferspeicher

geschrieben werden.

19. Verfahren nach mindestens einem der Ansprüche 13 bis 18, dadurch **gekennzeichnet**, dass ein Modus des eingebetteten Systems vorgesehen ist, in dem alle Schreib- und/oder Lesezugriffe der CPU auf das Kommunikationsmodul umgeleitet werden.

20. Verfahren nach mindestens einem der Ansprüche 13 bis 19, dadurch **gekennzeichnet**, dass ein Modus des eingebetteten Systems vorgesehen ist, in dem nur entweder die Schreibzugriffe oder die Lesezugriffe der CPU auf das Kommunikationsmodul umgeleitet werden, und die übrigen Zugriffe der CPU auf den Speicher von der CPU aktiv in den externen Speicher protokolliert werden.

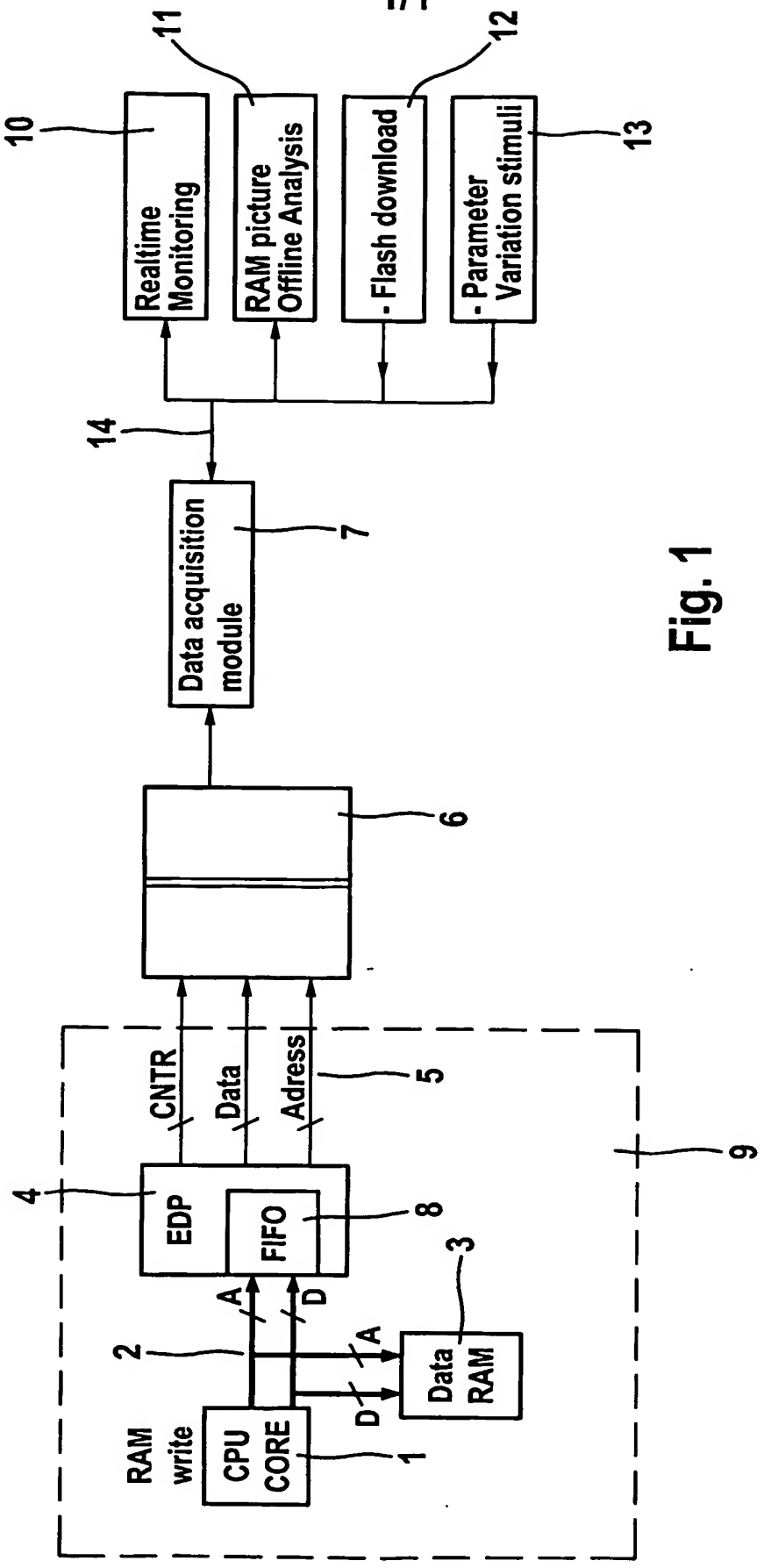

10
11
12
13
Realtime Monitoring
RAM picture Offline Analysis
- Flash download
- Parameter Variation stimuli
14
Data acquisition module
7
6
CNTR
Data
Adress
5
9
4
EDP
FIFO
8
3
A
D
2
A
D
Data RAM
RAM write
CPU CORE
1

Fig. 1